

Long Period Sequences Generated by the Logistic Map over Finite Fields with Control Parameter Four

Kazuyoshi Tsuchiya, and Yasuyuki Nogami

Abstract

Recently, binary sequences generated by chaotic maps have been widely studied. In particular, the logistic map is used as one of the chaotic map. However, if the logistic map is implemented by using finite precision computer arithmetic, rounding is required. In order to avoid rounding, Miyazaki, Araki, Uehara and Nogami proposed the logistic map over finite fields, and show some properties of sequences generated by the logistic map over finite fields. In this paper, we show some properties of periods of sequences generated by the logistic map over finite fields with control parameter four. In particular, we show conditions for parameters and initial values to have a long period, and asymptotic properties for periods by numerical experiments. Conditions for initial values are described by values of the Legendre symbol. The main idea is to introduce a structure of a hyperbola to certain sets of initial values. It follows that periods of sequences generated by the logistic map over finite fields on the sets of initial values are induced by periods of sequences generated by the square map on the parameter spaces of the hyperbola.

Index Terms

Hyperbola, Legendre symbol, logistic map over finite fields, long period sequences, square map.

I. INTRODUCTION

Recently binary sequences generated by chaotic maps have been widely studied. In particular, the logistic map is used as one of the chaotic map, which is defined by a polynomial of degree two over the interval $[0, 1]$. However, if the logistic map is implemented by using finite precision computer arithmetic, rounding is required. In order to avoid rounding, Miyazaki, Araki, Uehara and Nogami proposed the logistic map over a finite field (For details, see Section II).

This research was supported by KAKENHI Grant-in-Aid for Scientific Research (B) Number 25280047. This paper was presented in part at the seventh International Workshop on Signal Design and its Applications in Communications (IWSDA' 15), Indian Institute of Science, Bengaluru, India, September 2015.

K. Tsuchiya is with Kodan Electronics Co. Ltd., 2-13-24 Tamagawa, Ota-ku, Tokyo, Japan.

Y. Nogami is with the Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama-shi, Okayama, Japan.

Let p and \mathbb{F}_p be a prime number and the finite field with p elements, respectively. In [14] and [17], Miyazaki, Araki, Uehara and Nogami defined the logistic map over \mathbb{F}_p and studied sequences generated by the logistic map over \mathbb{F}_p . In [15], Miyazaki, Araki, Uehara and Nogami studied properties of sequences when p is a safe prime, where p is a safe prime (or 1-safe prime) if there is a prime number q such that $p = 2q + 1$. In [16], Miyazaki, Araki, Uehara and Nogami studied properties of sequences when p is a doubly safe prime, where a safe prime $p = 2q + 1$ is a doubly safe prime (or 2-safe prime) if q is a safe prime. In particular, they showed that there exists a sequence which has period length $(p - 3)/4$ by numerical experiments. In [17], Miyazaki, Araki, Uehara and Nogami showed the existence of an automorphism between two maps with different parameters. In [18], Miyazaki, Araki, Uehara and Nogami studied correlations for sequences.

The aim of this paper is to give some properties of periods of sequences generated by the logistic map over finite fields with control parameter four. We show conditions for parameters and initial values to have a long period. These conditions are weaker than the ones showed in [15] and [16]. Moreover we show asymptotic properties for periods by numerical experiments. Conditions for initial values are described by values of the Legendre symbol. The main idea is to introduce a structure of a hyperbola to certain sets of initial values.

On the other hand, we can regard sequences generated by the logistic map over finite fields as quadratic congruential pseudorandom number sequences modulo primes. Quadratic congruential generators are a type of nonlinear congruential pseudorandom number generators. As nonlinear congruential pseudorandom number generators, inversive congruential generators (Eichenauer and Lehn [8]) and power congruential generators (Lagarias [12], Lucheta, Miller and Reiter [13], Chou and Shparlinski [6]) have widely been studied (See Niederreiter [19]). Knuth [11] introduced quadratic congruential generators and showed the conditions for sequences which have a period of maximal length. Eichenauer and Lehn [9] studied the lattice structure of quadratic congruential pseudorandom number sequences. Blum, Blum and Shub [4], Rogers [21], Vasiga and Shallit [26], Somer and Krizek [24], Carlip and Mincheva [5] studied the simplest case, that is to say, the case of the iteration of the square map. Some other people have widely studied quadratic congruential generators (See Eichenauer-Herrmann, Herrmann and Wegenkittl [7], Strandt [25], Blažeková and Strauch [3], Blackburn, Gomez-Perez, Gutierrez and Shparlinski [2], Bauer, Vergnaud and Zapalowicz [1] and so on).

Now, we consider periods of quadratic congruential pseudorandom number sequences modulo odd primes p . Then there is no sequence which has a period of length p (See Knuth [11]). For the case that a recurrence polynomial is $f_0(z) = z^2 \in \mathbb{F}_p[z]$, Rogers [21] and Vasiga and Shallit [26] studied state diagrams of sequences in detail. Gilbert, Kolesar, Reiter and Storey [10] and Peinado, Montoya, Muñoz and Yuste [20] considered state diagrams of sequences for more general cases of $f_c(z) = z^2 + c \in \mathbb{F}_p[z]$. In particular, for the case of $f_{(-2)}(z) = z^2 - 2 \in \mathbb{F}_p[z]$, Vasiga and Shallit [26] studied state diagrams of sequences in detail. In fact a sequence generated by the logistic map over \mathbb{F}_p with control parameter four is transformed to a sequence defined by the polynomial $f_{(-2)}(z) = z^2 - 2$ by an automorphism. Thus one can have periods of sequences generated by the logistic map over \mathbb{F}_p with control parameter four by applying the results in Vasiga and Shallit [26]. Because they have an interest in graph theory for a state diagram of a sequence, they have considered not only long periods but also short periods. Thus they do

not specify sets of initial values in which an element generates a long period sequence. In this paper, we specify sets of initial values in which an element generates a long period sequence, and estimate periods on these sets by numerical experiments.

In Section II, we define the logistic map over finite fields and sequences generated by the logistic map over finite fields. In Section III, we introduce sets of initial values which generate long period sequences. In Section IV, we consider periods of sequences generated by the logistic map over finite fields. In Section V, we give some conditions for parameters to be maximal on the sets of initial values. In Section VI, we give some experimental results on periods of sequences.

We give some notations. For a prime number p , \mathbb{F}_p denotes the finite field with p elements. For a prime number p and an integer a , (a/p) denotes the Legendre symbol. For a finite set A , $\#A$ denotes the number of elements in A . For a finite field \mathbb{F}_p and the quadratic extension \mathbb{F}_{p^2} of \mathbb{F}_p , $N_{\mathbb{F}_{p^2}/\mathbb{F}_p} : \mathbb{F}_{p^2} \rightarrow \mathbb{F}_p$ denotes the norm map, namely, $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = \alpha\alpha^p$ for $\alpha \in \mathbb{F}_{p^2}$. For a finite extension of fields L/K and an algebraic variety X over L , $\text{Res}_{L/K} X$ denotes the Weil restriction. For a finite group G and an element $g \in G$, $\text{ord}_G(g)$ denotes the order of g in G . In particular, if G is the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ of the quotient ring $\mathbb{Z}/N\mathbb{Z}$ of integers modulo N , then we write $\text{ord}_N(g)$.

II. SEQUENCES GENERATED BY THE LOGISTIC MAP OVER FINITE FIELDS

In this section, we define the logistic map over finite fields, and sequences generated by the logistic map over finite fields.

Let p be a prime number, and $\mu_p \in \mathbb{F}_p - \{0\}$. We define a map $\text{LM}_{\mathbb{F}_p[\mu_p]} : \mathbb{F}_p \rightarrow \mathbb{F}_p$ as $\text{LM}_{\mathbb{F}_p[\mu_p]}(a) = \mu_p a(a+1)$ for any $a \in \mathbb{F}_p$ (Miyazaki, Araki, Uehara and Nogami [14] or [17]). The map $\text{LM}_{\mathbb{F}_p[\mu_p]}$ is called the logistic map over the finite field \mathbb{F}_p with control parameter μ_p . If $p > 3$ and $\mu_p = 4$, it is simply referred to as $\text{LM}_{\mathbb{F}_p}$.

Assume that $p > 3$. For an element $X_0 \in \mathbb{F}_p$, we consider a sequence $\{X_i\}$ defined as the recurrence relation

$$X_{i+1} = \text{LM}_{\mathbb{F}_p}(X_i) \quad (i \geq 0). \quad (1)$$

Let $\{X_i\}$ be a sequence defined as the recurrence relation (1). Then there exists the least positive integer s such that $X_s \in \{X_0, \dots, X_{s-1}\}$. And, there exists the least non negative integer t such that $X_t = X_s$. If $t > 0$, $\{X_0, \dots, X_{t-1}\}$ is called a link of $\{X_i\}$, and $\ell(X_0) := t$ is called the link length of $\{X_i\}$. $\{X_t, \dots, X_{s-1}\}$ is called a period of $\{X_i\}$, and $c(X_0) := s - t$ is called the period length of $\{X_i\}$.

III. SETS OF INITIAL VALUES AND A STRUCTURE OF THE HYPERBOLA

Period length of a sequence generated by a polynomial of degree two over a finite prime field of odd characteristic p is not maximal, namely p (See Knuth [11]). So we have to consider initial values which generate long period sequences. In this section, we specify sets of initial values in which an element generates a long period sequence by dividing a finite field into subsets determined by values of the Legendre symbol. In order to analyze these sets, we introduce a structure of a hyperbola.

Throughout the paper, let $p > 3$ be a prime number and $\text{LM}_{\mathbb{F}_p}$ be the logistic map over \mathbb{F}_p with $\mu_p = 4$.

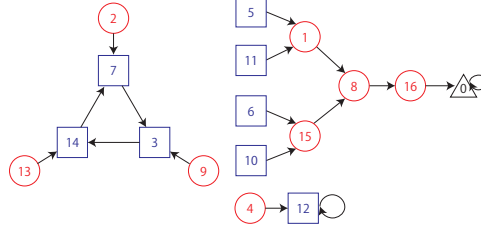


Fig. 1. The state diagram with informations on values of the Legendre symbol in the case of $p = 17$.

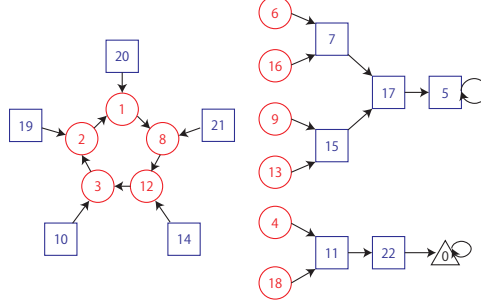


Fig. 2. The state diagram with informations on values of the Legendre symbol in the case of $p = 23$.

A. Observations

In order to obtain conditions for sets of initial values, we observe examples of sequences defined as the recurrence relation (1).

Example 1: Fig. 1 (resp. Fig. 2) describes the state diagram of the sequence defined as the recurrence relation (1) in the case of $p = 17$ (resp. $p = 23$). Here, an integer a in the circle means that $(a/p) = 1$, an integer a in the rectangle means that $(a/p) = -1$ and an integer a in the triangle means that $a \equiv 0 \pmod{p}$.

It is observed that $\#\{\text{LM}_{\mathbb{F}_p}^{-1}(a)\} = 0$ if and only if $(a/p) \neq (\text{LM}_{\mathbb{F}_p}(a)/p)$ for $a \in \mathbb{F}_p - \{-1\}$. In the case of $p = 17$ (resp. $p = 23$), an element $a \in \mathbb{F}_p$ such that $(a/p) = (\text{LM}_{\mathbb{F}_p}(a)/p) = -1$ (resp. $(a/p) = (\text{LM}_{\mathbb{F}_p}(a)/p) = 1$) generates a sequence of long period. Note that $17 \equiv 1 \pmod{4}$ and $23 \equiv 3 \pmod{4}$.

B. Sets of initial values

Now, we show properties of sequences defined as the recurrence relation (1) under general assumptions.

Lemma 2: Let $a \in \mathbb{F}_p$.

- 1) $\#\{\text{LM}_{\mathbb{F}_p}^{-1}(a)\} = 2$ if and only if $(a/p) = (\text{LM}_{\mathbb{F}_p}(a)/p)$.
- 2) $\#\{\text{LM}_{\mathbb{F}_p}^{-1}(a)\} = 1$ if and only if $a = -1$.
- 3) Assume that $a \neq -1$. Then $\#\{\text{LM}_{\mathbb{F}_p}^{-1}(a)\} = 0$ if and only if $(a/p) \neq (\text{LM}_{\mathbb{F}_p}(a)/p)$.

Proof: For $a \in \mathbb{F}_p$, the discriminant of the polynomial $4x(x+1) - a$ is $D := 16(a+1)$. Hence the statement follows from $(\text{LM}_{\mathbb{F}_p}(a)/p) = (a/p)(D/p)$. ■

For $s_0, s_1 \in \{\pm 1\}$, we define

$$\text{QHyp}[s_0, s_1] = \left\{ a \in \mathbb{F}_p \mid \left(\frac{a}{p} \right) = s_0, \left(\frac{a+1}{p} \right) = s_1 \right\}.$$

By Lemma 2, every element in $\text{QHyp}[-1, 1]$ or $\text{QHyp}[1, 1]$ has an inverse image of $\text{LM}_{\mathbb{F}_p}$. That is to say, these elements are candidates for being in periods.

Lemma 3: Let $a \in \text{QHyp}[-1, 1]$ or $a \in \text{QHyp}[1, 1]$. Put $\{c_1, c_2\} = \text{LM}_{\mathbb{F}_p}^{-1}(a)$.

1) If $p \equiv 1 \pmod{4}$ and $a \in \text{QHyp}[-1, 1]$, then $(c_1/p) \neq (c_2/p)$.

2) If $p \equiv 3 \pmod{4}$ and $a \in \text{QHyp}[1, 1]$, then $(c_1/p) \neq (c_2/p)$.

Proof: Since $4x(x+1) - a = 4(x-c_1)(x-c_2)$, $-a = 4c_1c_2$. Hence we have

$$\left(\frac{c_1}{p} \right) \left(\frac{c_2}{p} \right) = \left(\frac{-1}{p} \right) \left(\frac{a}{p} \right).$$

The statement follows from the first supplement to quadratic reciprocity. ■

By Lemma 3, if $p \equiv 1 \pmod{4}$ (resp. $p \equiv 3 \pmod{4}$), then every element in $\text{QHyp}[-1, 1]$ (resp. $\text{QHyp}[1, 1]$) is in a period. So one can expect that an element which holds the conditions in Lemma 3 generates a sequence of long period.

C. A structure of the hyperbola

In order to analyze $\text{QHyp}[s_0, s_1]$, we introduce a structure of a hyperbola. Let C be the hyperbola over \mathbb{F}_p defined by the equation $x^2 - y^2 = 1$. For an extension field K/\mathbb{F}_p , $C(K)$ denotes the set of K -rational points on C . Then we have a bijective map $\psi_K : K - \{0\} \rightarrow C(K)$ defined as $\psi_K(t) = (2^{-1}(t + t^{-1}), 2^{-1}(t - t^{-1}))$ for any $t \in K - \{0\}$ (See Silverman [23, I.1.3.1]).

Assume that $p \equiv 1 \pmod{4}$. Let $\pm i \in \mathbb{F}_p$ such that $(\pm i)^2 = -1$. For $s_0, s_1 \in \{\pm 1\}$, we define $\text{Param}_1[s_0, s_1]$ as

$$\text{Param}_1[1, 1] = \mathbb{F}_p - \{0, \pm 1, \pm i\},$$

$$\text{Param}_1[-1, 1] = \{t \in \mathbb{F}_{p^2} \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t) = 1\} - \{\pm 1\},$$

$$\text{Param}_1[1, -1] = \{t \in \mathbb{F}_{p^2} \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t) = -1\} - \{\pm i\},$$

$$\text{Param}_1[-1, -1] = \{t \in \mathbb{F}_{p^2} \mid t \notin \mathbb{F}_p, t^2 \in \mathbb{F}_p\}.$$

For $s_0, s_1 \in \{\pm 1\}$, we define $\Phi_1[s_0, s_1] : \text{Param}_1[s_0, s_1] \rightarrow \text{QHyp}[s_0, s_1]$ as $\Phi_1[s_0, s_1](t) = \{2^{-1}(t - t^{-1})\}^2$ for any $t \in \text{Param}_1[s_0, s_1]$.

Assume that $p \equiv 3 \pmod{4}$. Let $\pm \iota \in \mathbb{F}_{p^2} - \mathbb{F}_p$ such that $(\pm \iota)^2 = -1$. For $s_0, s_1 \in \{\pm 1\}$, we define $\text{Param}_3[s_0, s_1]$ as

$$\text{Param}_3[1, 1] = \mathbb{F}_p - \{0, \pm 1\},$$

$$\text{Param}_3[-1, 1] = \{t \in \mathbb{F}_{p^2} \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t) = 1\} - \{\pm 1, \pm \iota\},$$

$$\text{Param}_3[1, -1] = \{t \in \mathbb{F}_{p^2} - \mathbb{F}_p \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t) = -1\},$$

$$\text{Param}_3[-1, -1] = \{t \in \mathbb{F}_{p^2} \mid t \notin \mathbb{F}_p, t^2 \in \mathbb{F}_p\} - \{\pm \iota\}.$$

For $s_0, s_1 \in \{\pm 1\}$, we define $\Phi_3[s_0, s_1] : \text{Param}_3[s_0, s_1] \rightarrow \text{QHyp}[s_0, s_1]$ as $\Phi_3[s_0, s_1](t) = \{2^{-1}(t - t^{-1})\}^2$ for any $t \in \text{Param}_3[s_0, s_1]$.

Proposition 4: Let $p > 3$ be a prime number. Assume that $p \equiv j \pmod{4}$ ($j \in \{1, 3\}$). For $s_0, s_1 \in \{\pm 1\}$, $\Phi_j[s_0, s_1]$ is four-to-one map.

Proof: First we consider the case of $(s_0, s_1) = (1, 1)$. Let $a \in \text{QHyp}[1, 1]$. Then there are $b, c \in \mathbb{F}_p$ such that $a = b^2$ and $a + 1 = c^2$. Hence $(c, b) \in C(\mathbb{F}_p)$. Since $a \neq 0$, $b \neq 0$. If $p \equiv 1 \pmod{4}$, then $(0, \pm i) \in C(\mathbb{F}_p)$. Since $a + 1 \neq 0$, $(0, \pm i)$ do not correspond to elements in $\text{QHyp}[1, 1]$. Hence we have four-to-one map $\Phi_j[1, 1]$ for $j \in \{1, 3\}$.

Next we consider the case of $(s_0, s_1) = (-1, 1)$. Let $a \in \text{QHyp}[-1, 1]$. Then there are $\beta \in \mathbb{F}_{p^2} - \mathbb{F}_p$ and $c \in \mathbb{F}_p$ such that $a = \beta^2$ and $a + 1 = c^2$. Hence $(c, \beta) \in \{(x_0, y_0) \in C(\mathbb{F}_{p^2}) \mid x_0 \in \mathbb{F}_p, y_0 \in \mathbb{F}_{p^2} - \mathbb{F}_p\}$. If $p \equiv 3 \pmod{4}$, then $(0, \pm i)$ do not correspond to elements in $\text{QHyp}[-1, 1]$. Now, we have

$$\begin{aligned} & \{t \in \mathbb{F}_{p^2} \mid t + t^{-1} \in \mathbb{F}_p, t - t^{-1} \in \mathbb{F}_{p^2} - \mathbb{F}_p\} \\ &= \{t \in \mathbb{F}_{p^2} - \mathbb{F}_p \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t) = 1\}. \end{aligned}$$

Note that $t \in \mathbb{F}_p$ and $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t) = 1$ if and only if $t = \pm 1$. Hence we have four-to-one map $\Phi_j[-1, 1]$ for $j \in \{1, 3\}$.

For the case of $(s_0, s_1) = (1, -1)$, we may consider $\{(x_0, y_0) \in C(\mathbb{F}_{p^2}) \mid x_0 \in \mathbb{F}_{p^2} - \mathbb{F}_p, y_0 \in \mathbb{F}_p\}$. Similarly, we have four-to-one map $\Phi_j[1, -1]$ for $j \in \{1, 3\}$.

Finally we consider the case of $(s_0, s_1) = (-1, -1)$. Let $a \in \text{QHyp}[-1, -1]$. Then there are $\beta, \gamma \in \mathbb{F}_{p^2} - \mathbb{F}_p$ such that $a = \beta^2$ and $a + 1 = \gamma^2$. Hence $(\gamma, \beta) \in \{(x_0, y_0) \in C(\mathbb{F}_{p^2}) \mid x_0, y_0 \in \mathbb{F}_{p^2} - \mathbb{F}_p, x_0^2, y_0^2 \in \mathbb{F}_p\}$. Note that

$$\begin{aligned} & \{t \in \mathbb{F}_{p^2} \mid t \pm t^{-1} \in \mathbb{F}_{p^2} - \mathbb{F}_p, t^2 + t^{-2} \in \mathbb{F}_p\} \\ &= \{t \in \mathbb{F}_{p^2} \mid t \notin \mathbb{F}_p, t^2 \in \mathbb{F}_p, N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t) \neq \pm 1\}. \end{aligned}$$

Hence we have four-to-one map $\Phi_j[-1, -1]$ for $j \in \{1, 3\}$. ■

Remark 5: For any s_0, s_1, j , we have

$$\begin{aligned} \Phi_j[s_0, s_1](t) &= \Phi_j[s_0, s_1](-t) \\ &= \Phi_j[s_0, s_1](t^{-1}) = \Phi_j[s_0, s_1](-t^{-1}). \end{aligned} \tag{2}$$

Corollary 6: Let $p > 3$ be a prime number. For $s_0, s_1 \in \{\pm 1\}$, the number of elements in $\text{QHyp}[s_0, s_1]$ is given as Table I.

By Corollary 6, if a sequence attains maximal period length on $\text{QHyp}[-1, 1]$ (resp. $\text{QHyp}[1, 1]$), then the sequence has period length $(p - 1)/4$ (resp. $(p - 3)/4$).

Remark 7: Let \mathbb{G}_m be the multiplicative group scheme and $T_2 = \text{Ker}[N_{\mathbb{F}_{p^2}/\mathbb{F}_p} : \text{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p} \mathbb{G}_m \rightarrow \mathbb{G}_m]$ the norm

TABLE I
THE NUMBER OF ELEMENTS IN $\text{QHyp}[s_0, s_1]$

(s_0, s_1)	$(1, 1)$	$(-1, 1)$	$(1, -1)$	$(-1, -1)$
$p \equiv 1 \pmod{4}$	$(p-5)/4$	$(p-1)/4$	$(p-1)/4$	$(p-1)/4$
$p \equiv 3 \pmod{4}$	$(p-3)/4$	$(p-3)/4$	$(p+1)/4$	$(p-3)/4$

one torus (For details, see Waterhouse [28], Voskresenskii [27] and Rubin and Silverberg [22]). Then we have

$$\text{Param}_1[1, 1] = \mathbb{G}_m(\mathbb{F}_p) - \{\pm 1, \pm i\},$$

$$\text{Param}_3[1, 1] = \mathbb{G}_m(\mathbb{F}_p) - \{\pm 1\},$$

$$\text{Param}_1[-1, 1] = T_2(\mathbb{F}_p) - \{\pm 1\},$$

$$\text{Param}_3[-1, 1] = T_2(\mathbb{F}_p) - \{\pm 1, \pm i\}.$$

Thus, they have a common structure of a set of \mathbb{F}_p -rational points on an algebraic torus of dimension one except elements of order 1, 2 and 4.

IV. THE SQUARE MAPS AND PERIODS OF SEQUENCES

In this section, we consider periods of sequences generated by the logistic map over finite fields with control parameter four. For understanding periods, we relate the logistic map on the sets of initial values and the square map on the parameter spaces of the hyperbola.

A. The logistic map and the square map

Now, we relate the logistic map on the sets of initial values and the square map on the parameter spaces of the hyperbola.

Assume that $p \equiv 1 \pmod{4}$. Put

$$\text{Param}_1^+[1, 1] = \text{Param}_1[1, 1] \cup \{\pm i\},$$

$$\text{QHyp}^+[1, 1] = \text{QHyp}[1, 1] \cup \{-1\}.$$

We define $\Phi_1^+[1, 1] : \text{Param}_1^+[1, 1] \rightarrow \text{QHyp}^+[1, 1]$ as $\Phi_1^+[1, 1](t) = \{2^{-1}(t - t^{-1})\}^2$ for any $t \in \text{Param}_1^+[1, 1]$.

We define

$$\text{Sq}_1[1, 1] : \text{Param}_1[1, 1] \rightarrow \text{Param}_1^+[1, 1],$$

$$\text{Sq}_1[-1, 1] : \text{Param}_1[-1, 1] \rightarrow \text{Param}_1[-1, 1],$$

$$\text{Sq}_1[1, -1] : \text{Param}_1[1, -1] \rightarrow \text{Param}_1[-1, 1],$$

$$\text{Sq}_1[-1, -1] : \text{Param}_1[-1, -1] \rightarrow \text{Param}_1^+[1, 1]$$

as the square maps, that is to say, $\text{Sq}_1[s_0, s_1](t) = t^2$ for $s_0, s_1 \in \{\pm 1\}, t \in \text{Param}_1[s_0, s_1]$.

Lemma 8: Assume that $p \equiv 1 \pmod{4}$.

- 1) $\text{LM}_{\mathbb{F}_p}(\Phi_1[1, 1](t)) = \Phi_1^+[1, 1](\text{Sq}_1[1, 1](t))$ for any $t \in \text{Param}_1[1, 1]$.
- 2) $\text{LM}_{\mathbb{F}_p}(\Phi_1[-1, 1](t)) = \Phi_1[-1, 1](\text{Sq}_1[-1, 1](t))$ for any $t \in \text{Param}_1[-1, 1]$.
- 3) $\text{LM}_{\mathbb{F}_p}(\Phi_1[1, -1](t)) = \Phi_1[-1, 1](\text{Sq}_1[1, -1](t))$ for any $t \in \text{Param}_1[1, -1]$.
- 4) $\text{LM}_{\mathbb{F}_p}(\Phi_1[-1, -1](t)) = \Phi_1^+[1, 1](\text{Sq}_1[-1, -1](t))$ for any $t \in \text{Param}_1[-1, -1]$.

Proof: One can show the statement by similar argument in the proof of Lemma 9 below. ■

Assume that $p \equiv 3 \pmod{4}$. Put

$$\text{Param}_3^+[-1, 1] = \text{Param}_3[-1, 1] \cup \{\pm i\},$$

$$\text{QHyp}^+[-1, 1] = \text{QHyp}[-1, 1] \cup \{-1\}.$$

We define a map $\Phi_3^+[-1, 1] : \text{Param}_3^+[-1, 1] \rightarrow \text{QHyp}^+[-1, 1]$ as $\Phi_3^+[-1, 1](t) = \{2^{-1}(t - t^{-1})\}^2$ for any $t \in \text{Param}_3^+[-1, 1]$. We define

$$\text{Sq}_3[1, 1] : \text{Param}_3[1, 1] \rightarrow \text{Param}_3[1, 1],$$

$$\text{Sq}_3[-1, 1] : \text{Param}_3[-1, 1] \rightarrow \text{Param}_3^+[-1, 1],$$

$$\text{Sq}_3[1, -1] : \text{Param}_3[1, -1] \rightarrow \text{Param}_3^+[-1, 1],$$

$$\text{Sq}_3[-1, -1] : \text{Param}_3[-1, -1] \rightarrow \text{Param}_3[1, 1]$$

as the square maps, that is to say, $\text{Sq}_3[s_0, s_1](t) = t^2$ for $s_0, s_1 \in \{\pm 1\}, t \in \text{Param}_3[s_0, s_1]$.

Lemma 9: Assume that $p \equiv 3 \pmod{4}$.

- 1) $\text{LM}_{\mathbb{F}_p}(\Phi_3[1, 1](t)) = \Phi_3[1, 1](\text{Sq}_3[1, 1](t))$ for any $t \in \text{Param}_3[1, 1]$.
- 2) $\text{LM}_{\mathbb{F}_p}(\Phi_3[-1, 1](t)) = \Phi_3^+[-1, 1](\text{Sq}_3[-1, 1](t))$ for any $t \in \text{Param}_3[-1, 1]$.
- 3) $\text{LM}_{\mathbb{F}_p}(\Phi_3[1, -1](t)) = \Phi_3^+[-1, 1](\text{Sq}_3[1, -1](t))$ for any $t \in \text{Param}_3[1, -1]$.
- 4) $\text{LM}_{\mathbb{F}_p}(\Phi_3[-1, -1](t)) = \Phi_3[1, 1](\text{Sq}_3[-1, -1](t))$ for any $t \in \text{Param}_3[-1, -1]$.

Proof: Let $t \in \text{Param}_3[1, 1]$ and put $a = \Phi_3[1, 1](t) \in \text{QHyp}[1, 1]$. Then we have

$$\begin{aligned} & \text{LM}_{\mathbb{F}_p}(\Phi_3[1, 1](t)) \\ &= 4a(a + 1) \\ &= 4 \times \{2^{-1}(t - t^{-1})\}^2 \times \{2^{-1}(t + t^{-1})\}^2 \\ &= \{2^{-1}(t^2 - t^{-2})\}^2 \\ &= \Phi_3[1, 1](\text{Sq}_3[1, 1](t)). \end{aligned}$$

For the other cases, one can show the statement similarly. ■

Lemma 8 and Lemma 9 follow that periods of sequences generated by the logistic map over finite fields on the sets of initial values are induced by periods of sequences generated by the square map on the parameter spaces of the hyperbola. The latter has been studied by Rogers [21] and Vasiga and Shallit [26].

B. Periods of sequences

We consider periods of sequences generated by the logistic map over finite fields with control parameter four. First we give formulae for a link length and a period length of a sequence.

Theorem 10: Let $p > 3$ be a prime number. Assume that $p \equiv j \pmod{4}$ ($j \in \{1, 3\}$). Let $\{X_i\}$ be a sequence defined as the recurrence relation (1) with $X_0 \in \text{QHyp}[1, 1]$ (resp. $X_0 \in \text{QHyp}[-1, 1]$). Let $t \in \text{Param}_j[1, 1]$ (resp. $t \in \text{Param}_j[-1, 1]$) such that $\Phi_j[1, 1](t) = X_0$ (resp. $\Phi_j[-1, 1](t) = X_0$). Suppose that $\text{ord}_p(t) = 2^e d$ (resp. $\text{ord}_{T_2(\mathbb{F}_p)}(t) = 2^e d$), where d is an odd integer. Then the link length $\ell(X_0)$ of $\{X_i\}$ is given by

$$\ell(X_0) = \begin{cases} 0 & (e = 0) \\ e - 1 & (e > 0) \end{cases}, \quad (3)$$

and the period length $c(X_0)$ of $\{X_i\}$ is given by

$$c(X_0) = \begin{cases} \text{ord}_d(2) & (\nexists k \in \mathbb{Z} \text{ s.t. } 2^k \equiv -1 \pmod{d}) \\ \text{ord}_d(2)/2 & (\exists k \in \mathbb{Z} \text{ s.t. } 2^k \equiv -1 \pmod{d}) \end{cases}. \quad (4)$$

Proof: Note that the sequence $\{t^{2^i}\}$ has period length $\text{ord}_d(2)$ and link length e (Vasiga and Shallit [26, Theorem 1]). By (2), we have (4). Now, put $G = \mathbb{F}_p^\times$ (resp. $G = T_2(\mathbb{F}_p)$) if $X_0 \in \text{QHyp}[1, 1]$ (resp. $X_0 \in \text{QHyp}[-1, 1]$). Then, $\text{ord}_G(t) = d$ for some odd integer d if and only if $\text{ord}_G(-t) = 2d$ for some odd integer d . Hence we have (3). ■

Remark 11: If $\text{ord}_d(2)$ is an odd number, then there are no positive integers k such that $2^k \equiv -1 \pmod{d}$. When d is a prime number, $2^{(\text{ord}_d(2)/2)} \equiv -1 \pmod{d}$ if $\text{ord}_d(2)$ is an even integer.

Remark 12: In the case of $X_0 \in \text{QHyp}[1, -1]$ or $X_0 \in \text{QHyp}[-1, -1]$, we have $\ell(X_0) = \ell(\text{LM}_{\mathbb{F}_p}(X_0)) + 1$ and $c(X_0) = c(\text{LM}_{\mathbb{F}_p}(X_0))$.

Next, we show periods of sequences on $\text{QHyp}[1, 1]$ or $\text{QHyp}[-1, 1]$. In particular, we deal with periods of sequences that hold the conditions in Lemma 3.

Theorem 13: Let $p > 3$ be a prime number. Assume that $p \equiv 3 \pmod{4}$ (resp. $p \equiv 1 \pmod{4}$). Suppose that $p - 1 = 2m$ (resp. $p + 1 = 2m$), where m is an odd integer. Then, for any divisor $d \neq 1$ of m , the state diagram given by $\text{LM}_{\mathbb{F}_p}$ consists of n_d periods of length c_d on $\text{QHyp}[1, 1]$ (resp. $\text{QHyp}[-1, 1]$). Here n_d is given by

$$n_d = \begin{cases} \varphi(d)/(2\text{ord}_d(2)) & (\nexists k \in \mathbb{Z} \text{ s.t. } 2^k \equiv -1 \pmod{d}) \\ \varphi(d)/\text{ord}_d(2) & (\exists k \in \mathbb{Z} \text{ s.t. } 2^k \equiv -1 \pmod{d}) \end{cases}, \quad (5)$$

and c_d is given by

$$c_d = \begin{cases} \text{ord}_d(2) & (\nexists k \in \mathbb{Z} \text{ s.t. } 2^k \equiv -1 \pmod{d}) \\ \text{ord}_d(2)/2 & (\exists k \in \mathbb{Z} \text{ s.t. } 2^k \equiv -1 \pmod{d}) \end{cases}, \quad (6)$$

where φ is Euler's totient function.

Proof: For any divisor d of m , the state diagram given by the square map consists of $\varphi(d)/\text{ord}_d(2)$ periods of length $\text{ord}_d(2)$ on $\text{Param}_3[1, 1]$ (resp. $\text{Param}_1[-1, 1]$) if $p \equiv 3 \pmod{4}$ (resp. $p \equiv 1 \pmod{4}$). For details, see Rogers [21, Theorem] or Vasiga and Shallit [26, Corollary 3].

Fix a divisor $d \neq 1$ of m .

Suppose that there is no integer $k \in \mathbb{Z}$ such that $2^k \equiv -1 \pmod{d}$. Then a period of length c_d on $\text{QHyp}[1, 1]$ (resp. $\text{QHyp}[-1, 1]$) corresponds to two periods of length $\text{ord}_d(2)$ on $\text{Param}_3[1, 1]$ (resp. $\text{Param}_1[-1, 1]$). Hence it follows that $n_d = \varphi(d)/(2\text{ord}_d(2))$ and $c_d = \text{ord}_d(2)$.

Suppose that there is an integer $k \in \mathbb{Z}$ such that $2^k \equiv -1 \pmod{d}$. Then a period of length c_d on $\text{QHyp}[1, 1]$ (resp. $\text{QHyp}[-1, 1]$) corresponds to a period of length $\text{ord}_d(2)$ on $\text{Param}_3[1, 1]$ (resp. $\text{Param}_1[-1, 1]$). By (2), it follows that $n_d = \varphi(d)/\text{ord}_d(2)$ and $c_d = \text{ord}_d(2)/2$. ■

Remark 14: A sequence defined as the recurrence relation (1) is transformed to a sequence defined by the polynomial $z^2 - 2 \in \mathbb{F}_p[z]$ by an automorphism. The latter has been studied in great detail by Vasiga and Shallit [26]. So one can have Theorem 10 and Theorem 13 by applying the results in Vasiga and Shallit [26]. Because they have an interest in graph theory for a state diagram of a sequence, they have considered not only long periods but also short periods. On the other hand, we specified the sets $\text{QHyp}[1, 1]$ and $\text{QHyp}[-1, 1]$ of initial values in which an element generates a sequence of long period. Moreover we estimate periods on $\text{QHyp}[1, 1]$ and $\text{QHyp}[-1, 1]$ below. We consider periods by using a structure of the hyperbola. Vasiga and Shallit consider periods by using the Dickson polynomial.

V. LONG PERIOD SEQUENCES

Applying the logistic map over finite fields to a pseudorandom number generator, we need long period sequences. In this section, we give the conditions for parameters to be maximal on the sets of initial values. Moreover, we consider parallel generation of sequences.

A. Maximal sequences on the sets of initial values

Conditions for parameters to be maximal on the sets of initial values are deduced from (4).

Corollary 15: Let $q > 2$ be a prime number such that $p := 2q + 1$ (resp. $p := 2q - 1$) is a prime number. Assume that

$$\text{ord}_q(2) = q - 1 \tag{7}$$

or

$$\begin{cases} \text{ord}_q(2) = (q - 1)/2 \\ (q - 1)/2 \text{ is an odd integer.} \end{cases} \tag{8}$$

Let $\{X_i\}$ be a sequence defined as the recurrence relation (1) with $X_0 \in \text{QHyp}[1, 1]$ (resp. $X_0 \in \text{QHyp}[-1, 1]$). Then the sequence $\{X_i\}$ has period length $c(X_0) = (q - 1)/2$.

Remark 16: For a prime number p , p is a safe prime (or 1-safe prime) if there is a prime number q with $p = 2q + 1$. If $q > 2$, then $p \equiv 3 \pmod{4}$ and $(q - 1)/2 = (p - 3)/4$. For a safe prime $p = 2q + 1$, p is a doubly safe prime (or 2-safe prime) if q is a safe prime. If $p = 2q + 1$ is a doubly safe prime, then q holds (7) or (8). Peinado, Montoya, Muñoz and Yuste [20, Remark 2] and Miyazaki, Araki, Uehara and Nogami [16] considered in this situation.

A prime number p is a maximal prime on $\text{QHyp}[1, 1]$ (resp. $\text{QHyp}[-1, 1]$) if there is a prime number $q > 2$ such that $p = 2q + 1$ (resp. $p = 2q - 1$) and q holds (7) or (8).

B. Parallel generation of sequences

In the case of non-maximal sequences, there are at least two periods. If we can select two initial values which generate two different periods each other, we can generate two sequences in parallel, which have no collisions.

Corollary 17: Let $q_1, q_2 > 2$ be different prime numbers such that $p := 2q_1q_2 + 1$ (resp. $p := 2q_1q_2 - 1$) is a prime number. For any $i \in \{1, 2\}$, assume that

$$\text{ord}_{q_i}(2) = q_i - 1$$

or

$$\begin{cases} \text{ord}_{q_i}(2) = (q_i - 1)/2 \\ (q_i - 1)/2 \text{ is an odd integer.} \end{cases}$$

Let ω be a primitive element of \mathbb{F}_p (resp. ω_0 be a primitive element of \mathbb{F}_{p^2} and $\omega = \omega_0^{p-1}$). Put $t_1 = \omega^{2q_2}, t_2 = \omega^{2q_1}$. Put $X_0 = \Phi_3[1, 1](t_1), Y_0 = \Phi_3[1, 1](t_2)$ (resp. $X_0 = \Phi_1[-1, 1](t_1), Y_0 = \Phi_1[-1, 1](t_2)$). Let $\{X_i\}$ and $\{Y_i\}$ be sequences defined as the recurrence relation (1) with initial values X_0 and Y_0 , respectively. Then the sequence $\{X_i\}$ has period length $c(X_0) = (q_1 - 1)/2$ and the sequence $\{Y_i\}$ has period length $c(Y_0) = (q_2 - 1)/2$.

Remark 18: By adding the condition $((q_1 - 1)/2, (q_2 - 1)/2) = 1$, we can obtain highly independent sequences.

Remark 19: If the size of q_1 and q_2 are the same, then the size of p is about twice.

VI. NUMERICAL EXPERIMENTS

One can expect that a sequence generated by the logistic map over a finite field \mathbb{F}_p on $\text{QHyp}[-1, 1]$ (resp. $\text{QHyp}[1, 1]$) has a long period if $p \equiv 1 \pmod{4}$ (resp. $p \equiv 3 \pmod{4}$). In this section, we estimate a ratio of maximal primes, the number of periods and period lengths on the sets of initial values.

Fix a positive integer n .

Now, for $3 \leq n \leq 32$, we show the number of n -bit primes p with $p \equiv 1 \pmod{4}$, the number of n -bit primes p with $p \equiv 3 \pmod{4}$, the ratio of n -bit maximal primes on $\text{QHyp}[-1, 1]$ in n -bit primes p with $p \equiv 1 \pmod{4}$ and the ratio of n -bit maximal primes on $\text{QHyp}[1, 1]$ in n -bit primes p with $p \equiv 3 \pmod{4}$ in Table II, and the graph of the ratio of maximal primes on $\text{QHyp}[-1, 1]$ and $\text{QHyp}[1, 1]$ in Fig. 3. Table II and Fig. 3 show that both ratios are slowly decreasing and that the ratio of n -bit maximal primes on $\text{QHyp}[-1, 1]$ in n -bit primes p with $p \equiv 1 \pmod{4}$ is smaller than the ratio of n -bit maximal primes on $\text{QHyp}[1, 1]$ in n -bit primes p with $p \equiv 3 \pmod{4}$. This means that the order of 2 in \mathbb{F}_q where $p = 2q + 1$ tends to be larger than the order of 2 in \mathbb{F}_q where $p = 2q - 1$. The cause is not clear.

This observation shows that maximal primes are rare. Therefore we estimate the number of periods and period lengths on the sets of initial values by applying (5) and (6). In Table III, for $3 \leq n \leq 32$, we show the average

TABLE II
THE NUMBER OF PRIMES AND THE RATIO OF MAXIMAL PRIMES

n	the number of primes		the ratio of maximal primes (%)	
	$p \equiv 1 \pmod{4}$	$p \equiv 3 \pmod{4}$	$p \equiv 1 \pmod{4}$	$p \equiv 3 \pmod{4}$
3	1	1	100.0	100.0
4	1	1	100.0	100.0
5	2	3	0.0	33.3
6	4	3	25.0	66.7
7	6	7	16.7	14.3
8	10	13	10.0	7.7
9	21	22	14.3	22.7
10	38	37	7.9	16.2
11	66	71	10.6	7.0
12	127	128	5.5	10.9
13	233	231	8.2	12.1
14	432	440	8.1	9.5
15	805	807	7.0	9.3
16	1511	1519	5.8	8.2
17	2837	2872	5.7	8.3
18	5378	5371	5.1	7.9
19	10186	10204	4.8	7.1
20	19294	19341	4.4	6.6
21	36827	36759	4.2	6.5
22	70157	70179	4.2	6.1
23	133975	134241	3.9	5.8
24	256852	256856	3.7	5.5
25	492882	492936	3.6	5.3
26	946848	947272	3.4	5.1
27	1823129	1822615	3.3	4.9
28	3513599	3513691	3.1	4.7
29	6780412	6781495	3.0	4.5
30	13103462	13103816	2.9	4.4
31	25348870	25348667	2.8	4.2
32	49090415	49092241	2.7	4.1

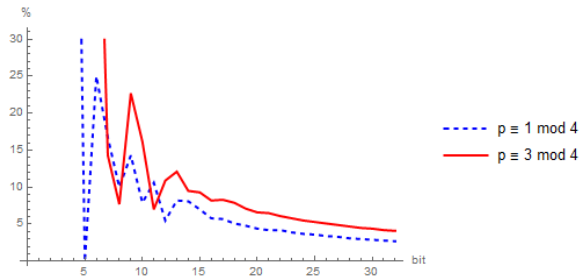


Fig. 3. The graph of the ratio of maximal primes.

of the number of periods and of the period lengths on $\text{QHyp}[-1, 1]$ (resp. $\text{QHyp}[1, 1]$) in n -bit primes p with $p \equiv 1 \pmod{4}$ (resp. $p \equiv 3 \pmod{4}$). For $17 \leq n \leq 32$, we show the graph of the average of the number of periods in Fig. 4 and the graph of the average of period lengths in Fig. 5. Table III, Fig. 4 and Fig. 5 show that both averages of the number of periods and of period lengths are increasing rapidly. As in Fig. 3, the average of period lengths in the case of $p \equiv 1 \pmod{4}$ is smaller than the average of period lengths in the case of $p \equiv 3 \pmod{4}$. On the other hand, the average of the number of periods in the case of $p \equiv 1 \pmod{4}$ is almost the same as the average of the number of periods in the case of $p \equiv 3 \pmod{4}$.

TABLE III
THE AVERAGE OF THE NUMBER OF PERIODS AND PERIOD LENGTHS

n	the average of the number of periods		the average of period lengths	
	$p \equiv 1 \pmod{4}$	$p \equiv 3 \pmod{4}$	$p \equiv 1 \pmod{4}$	$p \equiv 3 \pmod{4}$
3	1.00000	1.00000	1.00000	1.00000
4	1.00000	1.00000	3.00000	2.00000
5	2.50000	2.00000	2.16667	3.11111
6	2.50000	1.66667	5.41667	9.44444
7	3.33333	3.57143	9.23333	8.77551
8	3.80000	4.30769	16.9352	13.8487
9	6.04762	5.09091	28.7254	35.0402
10	7.76316	7.13514	43.7889	59.4553
11	9.10606	10.3380	97.0964	82.1112
12	12.6299	13.8438	147.783	180.139
13	16.1416	16.6926	301.326	358.324
14	21.9144	19.4182	591.330	650.540
15	26.5565	26.6183	1109.35	1223.50
16	35.9226	38.6781	2034.04	2216.20
17	47.6355	46.3492	3745.69	4348.82
18	62.6923	58.3020	6864.25	8273.57
19	82.7361	83.2753	13451.1	15339.2
20	108.124	107.706	25257.7	29159.2
21	143.124	139.198	48344.3	56612.0
22	186.104	183.434	94329.2	108324
23	251.771	244.311	180290	208554
24	324.754	327.949	345958	400562
25	433.381	431.324	670836	775057
26	578.287	570.413	1.29110×10^6	1.49509×10^6
27	758.097	761.405	2.50197×10^6	2.89141×10^6
28	1013.00	1007.39	4.85357×10^6	5.59784×10^6
29	1350.15	1336.60	9.41888×10^6	1.08625×10^7
30	1784.44	1787.59	1.83069×10^7	2.11058×10^7
31	2386.64	2373.55	3.56112×10^7	4.09809×10^7
32	3178.33	3179.42	6.93144×10^7	7.97218×10^7

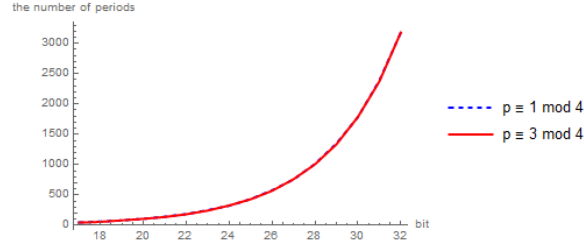


Fig. 4. The graph of the average of the number of periods.

VII. CONCLUSION

In this paper, we study periods of sequences generated by the logistic map over finite fields with control parameter four. The conditions for initial values are given by values of the Legendre symbol. It is crucial that periods of sequences generated by the logistic map over finite fields on the sets of initial values are induced by periods of sequences generated by the square map on the parameter spaces of the hyperbola. In particular, we show the conditions for parameters to be maximal on the sets of initial values, and estimate a ratio of maximal primes, the number of periods and period lengths on the sets of initial values.

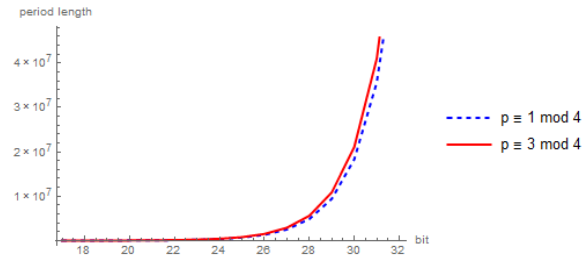


Fig. 5. The graph of the average of period lengths.

ACKNOWLEDGMENT

The authors would like to thank Satoshi Uehara, Shunsuke Araki and Takeru Miyazaki for useful discussion. In particular, the authors would like to thank Satoshi Uehara for his valuable comments.

REFERENCES

- [1] A. Bauer, D. Vergnaud and J. -C. Zapalowicz, “Inferring sequences produced by nonlinear pseudorandom number generators using Coppersmith’s methods,” in *Public key cryptography – PKC 2012, 15th Int. Conf. Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012, Proc.*, (Lecture Notes in Comput. Sci. 7293) Springer-Verlag Berlin Heidelberg, 2012, pp.609–626.
- [2] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, “Predicting nonlinear pseudorandom number generators,” *Math. Comput.*, vol. 74, pp.1471–1494, 2005.
- [3] O. Blažeková and O. Strauch, “Pseudo-randomness of quadratic generators,” *Uniform Distribution Theory*, vol. 2, pp.105–120, 2007.
- [4] L. Blum, M. Blum and M. Shub, “A simple unpredictable pseudo-random number generator,” *SIAM J. Comput.*, vol. 15, no. 2 pp.364–383, May 1986.
- [5] W. Carlip and M. Mincheva, “Component growth of iteration graphs under the squaring map modulo p^k ,” *Fibonacci Quart.*, vol. 45, no. 3 pp.239–246, Aug. 2007.
- [6] W. -S. Chou and I. E. Shparlinski, “On the cycle structure of repeated exponentiation modulo a prime,” *J. Number Theory*, vol. 107, pp.345–356, Aug. 2004.
- [7] J. Eichenauer-Herrmann, E. Herrmann and S. Wegenkittl, “A survey of quadratic and inversive congruential pseudorandom numbers,” in *Monte Carlo and Quasi-Monte Carlo methods 1996 Proc. conf. University of Salzburg, Austria, July 9-12, 1996*, (Lecture Notes in Statist. 127) New York, NY, USA: Springer-Verlag New York, 1998, pp.66–97.
- [8] J. Eichenauer and J. Lehn, “A non-linear congruential pseudo random number generator,” *Statistische Hefte*, vol. 27, pp.315–326, Dec. 1986.
- [9] J. Eichenauer and J. Lehn, “On the structure of quadratic congruential sequences,” *manuscripta math.*, vol. 58, pp.129–140, 1987.
- [10] C. L. Gilbert, J. D. Kolesar, C. A. Reiter and J. D. Storey, “Function digraphs of quadratic maps modulo p ,” *Fibonacci Quart.*, vol. 39, no. 1 pp.32–49, Feb. 2001.
- [11] D. E. Knuth, *The art of computer programming volume 2: Seminumerical algorithms*, 3rd ed. Boston, MA, USA: Addison-Wesley, 1997.
- [12] J. C. Lagarias, “Pseudorandom number generators in cryptography and number theory,” in *Cryptology and computational number theory*, (Proc. Symp. Appl. Math., vol. 42) Providence, RI, USA: Amer. Math. Soc., 1990, pp.115–143.
- [13] C. Lucheta, E. Miller and C. Reiter, “Digraphs from powers modulo p ,” *Fibonacci Quart.*, vol. 34, no. 3 pp.226–239, June–July 1996.
- [14] T. Miyazaki, S. Aarki, S. Uehara and Y. Nogami, “A study on the pseudorandom number generator for the logistic map over prime fields,” in *Proc. 30th Symp. Cryptography and Inform. Security*, Kyoto, 2013.(Japanese)
- [15] T. Miyazaki, S. Aarki, S. Uehara and Y. Nogami, “A study of the logistic map over prime fields with the safe prime,” in *Proc. 2013 Annu. Meeting Jpn. Soc. for Ind. and Appl. Math.*, Fukuoka, 2013.(Japanese)

- [16] T. Miyazaki, S. Aarki, S. Uehara and Y. Nogami, "A study of averages of periods for sequences generated by the logistic map over prime fields with the doubly safe prime," in *Proc. 31st Symp. Cryptography and Inform. Security*, Kagoshima, 2014.(Japanese)
- [17] T. Miyazaki, S. Aarki, S. Uehara and Y. Nogami, "A study of an automorphism on the logistic maps over prime fields," in *Proc. Int. Symp. Inform. Theory and Its Appl.*, Melbourne, 2014, pp.727–731.
- [18] T. Miyazaki, S. Aarki, S. Uehara and Y. Nogami, "Distribution of correlations for sequences generated by the logistic map over prime field," in *Proc. 32nd Symp. Cryptography and Inform. Security*, Kokura, 2015.(Japanese)
- [19] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, (CBMS-NSF regional conf. series in appl. math. : 63) Philadelphia, PA, USA: Soc. for Ind. and Appl. Math., 1992.
- [20] A. Peinado, F. Montoya, J. Muñoz and A. J. Yuste, "Maximal periods of $x^2 + c$ in \mathbb{F}_q ," in *Appl. Algebra, Algebraic Algorithms and Error-Correcting Codes 14th Int. Symp., AAECC-14, Melbourne, Australia, Nov. 26–30, 2001. Proc.*, (Lecture Notes in Comput. Sci. 2227) Springer-Verlag Berlin Heidelberg, 2001, pp.219–228.
- [21] T. D. Rogers, "The graph of the square mapping on the prime fields," *Discrete Math.*, vol. 148, pp.317–324, Jan. 1996.
- [22] K. Rubin and A. Silverberg, "Torus-based cryptography," in *Advances in cryptology –CRYPTO 2003, 23rd Annu. int. cryptology conf., Santa Barbara, California, USA, Aug. 17–21, 2003, Proc.*, (Lecture Notes in Comput. Sci. 2729) Springer-Verlag Berlin Heidelberg, 2003, pp.349–365.
- [23] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed. (Graduate Texts in Mathematics 106) New York, NY, USA: Springer-Verlag New York, 2009.
- [24] L. Somer and M. Křížek, "Structure of digraphs associated with quadratic congruences with composite moduli," *Discrete Math.*, vol. 306, pp.2174–2185, Sep. 2006.
- [25] S. Strandt, "Quadratic congruential generators with odd composite modulus," in *Monte Carlo and Quasi-Monte Carlo methods 1996 Proc. conf. University of Salzburg, Austria, July 9-12, 1996*, (Lecture Notes in Statist. 127) New York, NY, USA: Springer-Verlag New York, 1998, pp.415–426.
- [26] T. Vasiga and J. Shallit, "On the iteration of certain quadratic maps over $\text{GF}(p)$," *Discrete Math.*, vol. 277, pp.219–240, Feb. 2004.
- [27] V. E. Voskresenskii, *Algebraic groups and their birational invariants*, (Translations of mathematical monographs, vol. 179) Providence, RI, USA: Amer. Math. Soc., 1998.
- [28] W. C. Waterhouse, *Introduction to affine group schemes*, (Graduate Texts in Mathematics 66) New York, NY, USA: Springer-Verlag New York, 1979.